MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

TEH3221 – ETHICAL HACKING AND SECURITY ASSESSMENT

(All sections / Groups)

10 MARCH 2016
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 8 pages, excluding the cover page, with 10 MCQs and 6 questions only.

2. Attempt **ALL** questions in **Section A**.

3. Attempt **FIVE out of SIX** questions in **Section B**. All questions carry equal marks and the distribution of the marks for each question is given.

4. Please print all your answers in the Answer Booklet provided.

SECTION A: Please attempt **ALL** multiple choice questions. [10 marks]

1. In the _____ model, the company will provide a network diagram which showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs).
   a. black box
   b. white box
   c. tiger box
   d. gray box

2. In the TCP/IP stack, the _____ layer is where applications and protocols, such as HTTP and Telnet, operate.
   a. internet
   b. application
   c. transport
   d. network

3. _____ enables an attacker to join a TCP session and make both parties think he or she is the other party.
   a. DoS attack
   b. Session hijacking
   c. Ping of Death (PoD)
   d. Buffer overflow

4. _____ can be used to gather information useful for computer criminals, like company phone directories, financial reports, interoffice memos, etc.
   a. Piggybacking
   b. Dumpster diving
   c. Shoulder surfing
   d. Footprinting

5. During TCP three-way handshake, a computer that receives a SYN packet from a remote computer responds to the packet with a(n) _____ packet if its port is open.
   a. ACK
   b. SYN/ACK
   c. RST
   d. FIN

Continued .....

6. One of the biggest vulnerabilities of NetBIOS systems is a(n) _____, which is an unauthenticated connection to a Windows computer using no logon and password values.
   a. open session
   b. void session
   c. null session
   d. hijack session

7. Windows Server 2003 and 2008 _____ are used to authenticate user accounts, so they contain much of the information that attackers want to access.
   a. SMB controller
   b. CIFS servers
   c. domain controller
   d. Start of Authority (SOA) controller

8. Disgruntled employees might install a(n) _____ in company computers' flash memory before they leave a company and later use it to gain access to the corporate network.
   a. embedded keylogger
   b. unclassified kernel
   c. BIOS-based rootkit
   d. patch

9. SQL _____ involves the attacker supplying SQL commands when prompted to fill in a Web application field.
   a. spoofing
   b. redirection
   c. injection
   d. poisoning

10. _____ uses TLS to authenticate the server to the client but not the client to the server.
    a. PPP
    b. EAP
    c. PEAP
    d. EAP-TLS

Continued .....

SECTION B: Please attempt **FIVE** out of **SIX** questions only

Question 1:

a) Fill in the blanks with the most appropriate application layer service:

i. _____: The primary protocol used to communicate over the World Wide Web; usually associated with port 80.

ii. _____: Used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using an unencrypted virtual terminal connection; usually associated with port 23.

iii. _____: Communication protocol for mail servers to transmit email over the Internet; usually associated with port 25.

iv. _____: Primarily used to monitor devices on a network, such as remotely monitoring a router's state; usually associated with port 161 and 162.

v. _____: An encrypted network protocol which enables a remote user to log on to a server and issue commands; usually associated with port 22.

[5 marks]

b) Identify the **FOUR [4]** critical components of a TCP header. If you want to perform a session hijacking, which component you should pay attention to? Explain how you may abuse it.

[4 marks]

c) What is the most important recommendation that should be made to a client to help prevent viruses from being introduced into corporate network?

[1 mark]

Continued .....

Question 2:

a) `Backdoor.Slackbot.B` (a Trojan program) was programmed to control a computer by using Internet Relay Chat (IRC) on port 6667. Is this a good approach taken by computer criminals? Explain your answer.

[2 marks]

b) What is *Whois* utility? Explain how the computer criminals can use this utility for their evil purpose.

[2 marks]

c) Reported by Tripwire on year 2013, "*Google's Malaysian domains google.com.my and google.my were hijacked, redirecting users to a webpage that announced the attack was perpetrated by a Pakistani group called Madleets*". What is this attack? Explain your answer by providing **TWO [2]** preventive measures.

[6 marks]

Continued .....

Question 3:

a) What is the purpose of a Web bug (beacon)? How do they relate to or differ from spyware?

[3 marks]

b) Based on question 3(a), please suggest **TWO [2]** methods to prevent a web bug from tracking Internet activities.

[2 marks]

c) Based on the following scenarios, identify the best Nmap scan type and define the Nmap scan command parameter for each of them.

i. You do not have the raw packet privileges, and need to make Nmap to establish a connection with the target machine and port by issuing the `connect` system call.

ii. You want to remain stealthy and do not want the target machines to log the connection.

iii. You want to scan the systems compliant with RFC793 without utilizing any bit.

iv. You want to determine which hosts in a network are up by pinging them all.

v. You want to scan a target without sending a single packet from your own IP address.

[5 marks]

Continued .....

Question 4:

a) Refer to the table provided below, and answer the following questions:

Name	Number(h)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<\\--__MSBROWSE__>	01	G	Master Browser
<computername>	1F	U	NetDDE Service
<computername> Interchange(MSMail Connector)	22	U	Microsoft Exchange
<domain>	1C	G	Domain Controllers
<IS~computer name>	00	U	IIS
<computername>	[2B]	U	Lotus Notes Server Service
IRISMULTICAST	[2F]	G	Lotus Notes
Forte_$ND800ZA Service	[20]	U	DCA IrmaLan Gateway Server

i. If you are a hacker, which column of the table will get your attention? Why?

[2 marks]

ii. If you are a hacker, which machine will you target? Why?

[2 marks]

b) The Win32 class contains many functions you can call through a Perl script. How can attackers use these functions? As a security professional, should you become proficient at using them in a program?

[2 marks]

c) According to security services company Proofpoint's report dated on September 2015, *GreenDispenser* is a variant of the malware family that includes "*Suceful*", "*Plotus*" and "*Padpin*" (also known as *Tyupkin*). The malware has been coded to interact with the XFS middleware widely adopted by automated teller machine (ATM) makers.
Identify **FOUR [4]** functions that most ATM malwares can perform.

[4 marks]

Continued .....

Question 5:

a) Applying your Linux/ UNIX knowledge, answer all of the following by granting the correct permissions with octal representation.

i. To grant read, and write permission to the *Owner* of a file, and read permission to both of the *Group* and *Other*.

ii. To grant execute permission to the *Owner* of a file, write permission to *Group*, and no permissions to *Other*.

iii. A directory was created with default permission of octal 777, what is the umask value you should apply if you want to revoke the write permission from *Owner*, *Group* and *Other* on this directory?

iv. A directory was created with default permission of octal 777, what is the umask value you should apply if you want to revoke the execute permission from *Owner*, *Group* and *Other* on this directory?

v. A directory was created with default permission of octal 555. If you create a directory with a umask of octal 111, what effect does this have on the directory?

[5 marks]

b) What can be accomplished by typing the command of "`finger root`" in *nix systems?

[2 marks]

c) Outlined in the CVE-2015-2894, the popular sysadmin tool – *Up.Time* version 7.4 allowed an unauthenticated attacker on the network to send commands with an input which is larger than 1024 bytes, and eventually, will crash the application. Do you think it is a kind of buffer overflow? Explain your answer and suggest **TWO [2]** general ways to prevent this flaw.

[3 marks]

Continued .....

Question 6:

a) Hackers often set up rogue WiFi networks in popular tourist spots, airports, cafes, etc. and hoping to trap travelers who log in and are desperate for a connection. Do you think this technique is workable? What information can be extracted by hackers if the travelers log in to their fake Wi-Fi? Explain your answer in detail.

[4 marks]

b) What is war driving? One of the mandatory tools for war driving is *Wireshark*, is that true? Justify your answer.

[3 marks]

c) Refer to the result below, what is the hacker attempting to do? Analyze the result.

```
root@kali: nc -vv www.mmu.edu.my 80
192.168.21.11: inverse host lookup failed: Unknown server
error: Connection timed out
(Unknown) [192.168.21.11] 80 (www) open

GET HTTP
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.1
Date: Thu, 10 Dec 2015 12:00:00 GMT
Content-Type: text/html
Content-Length: 87
```

[3 marks]

End of Page